IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA v. ANTHONY AYEAH, MOUAAZ ELKHEBRI, ONYEWUCHI IBEH, and JASON JOYNER *Defendants*.	**UNDER SEAL** Case No. 1:21-mj-00279

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT AND ARREST WARRANT

I, Ethan Papish, Special Agent, being duly sworn, hereby, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am employed as a Special Agent of the United States Secret Service ("USSS") and have been so employed since 2017. I am currently assigned to the Washington Field Office, Cyber Fraud Task Force. My duties and responsibilities include the investigation of white collar and financial crimes such as identity theft and identity crimes, bank fraud, access device fraud, wire fraud, computer fraud, and forgery. I received training in conducting investigations into these criminal offenses as well as others. I am a graduate of the Special Agent Training Course at the USSS James J. Rowley Training Center and the Criminal Investigator Training Program at the Federal Law Enforcement Training Center. As a Special Agent, I am authorized to investigate violations of laws of the United States, and I am authorized to execute warrants issued under the authority of the United States.

2. This affidavit is based on my personal investigation and the investigation of others, including federal and local law enforcement officials whom I know to be reliable. The facts and information contained in this affidavit are based upon witness interviews and my review of records, documents, and other physical evidence obtained during this investigation. This affidavit does not include each and every fact known to the government, but only those facts necessary to support a finding of probable cause to support the requested Criminal Complaint. All dates in this affidavit are approximate.

3. I make this affidavit in support of a Criminal Complaint charging ANTHONY AYEAH ("AYEAH"); MOUAAZ ELKHEBRI ("ELKHEBRI"); ONYEWUCHI IBEH ("IBEH"); and JASON JOYNER ("JOYNER") (collectively, the "CONSPIRATORS") with, from on or about January 1, 2018, to on or about March 31, 2020, in the Eastern District of Virginia, and elsewhere, knowingly and intentionally conspiring with each other and with others, known and unknown, to commit wire fraud by knowingly devising and intending to devise a scheme and artifice to defraud and to obtain money by means of materially false and fraudulent pretenses, representations, and promises; and transmitting and causing to be transmitted interstate wire communications in furtherance of the conspiracy, contrary to Title 18, United States Code, Section 1343 and in violation of Title 18, United States Code, Section 1349.

PROBABLE CAUSE

A. The General Scheme to Defraud

4. In August 2019, the USSS and the United States Postal Inspection Service ("USPIS") initiated an investigation into an organized criminal enterprise engaged in schemes to defraud various U.S. banks and victim businesses (the "Joint Investigation"). This investigation

identified a business email compromise ("BEC") scheme using various U.S. banks and defrauding multiple victim businesses.

5. The CONSPIRATORS targeted victims in the United States and across the globe, including small and large businesses in various industries. Some of the victims of the conspiracy lost hundreds of thousands of dollars to these fraudulent schemes. The CONSPIRATORS targeted employees with access to company finances and trick them into making wire transfers to bank accounts thought to belong to legitimate business partners, when in fact, the money was fraudulently misdirected and deposited into accounts controlled by the CONSPIRATORS.

6. In typical BEC schemes, the perpetrators gain access to business networks through phishing attacks or the use of malware. Undetected, they may spend weeks or months studying each organization's vendors, billing systems, and the style of email communication between individuals responsible for making financial transactions. When the timing is right, often when a real transaction is due for payment, the scammers send a bogus email to a targeted employee in the finance office – a bookkeeper, accountant, controller, or chief financial officer. Often these emails may include correct invoices or other documentation and may come directly after a trusted vendor has requested payment and include the trusted vendor's correspondence in the email. The bogus email comes as a follow up to the request for payment, advising the targeted employee that the banking information for the trusted vendor has changed, usually from an email address disguised to look like the trusted vendor's real email address. The targeted employee believes he or she is sending money to the trusted vendor, just as he or she has done in the past. However, the updated banking information provided by the criminal group results in a transfer of what might be tens or hundreds of thousands of dollars to a different account controlled by the criminal group.

B. The Conspirators Defraud Victim-1.

7. On or about January 11, 2019,[1] a victim located in Boston, Massachusetts ("Victim-1"), filed a complaint stating that their business was defrauded of $356,954 on December 10, 2018. Falling victim to the BEC tactics described above, $356,954 was wired from Victim-1's HSBC Bank USA, N.A. account ending in -6572 (the "HSBC-6572 account") to a CONSPIRATOR-controlled Wells Fargo account ending in -9986 (the "WF-9986 account"). Victim-1 was tricked into believing the WF-9986 account was the legitimate account of their legitimate business partner. This information was confirmed on or about October 16, 2019, when the Joint Investigation interviewed Victim-1's President and Chief Financial Officer.

8. One aspect of the email deception was accomplished by the fraudsters registering domain names with misspellings (*i.e.* adding an additional letter) of both Victim-1's legitimate domain name and the legitimate domain name of their business partner. These look-a-like domains were used to communicate with the business partners. According to Victim-1, on December 5, 2018, the CONSPIRATOR-controlled look-a-like domain of their business partner was used to send an email to Victim-1 requesting the payment destination be changed to the WF-9986 account.

9. Records from Wells Fargo show that the account was opened by Uncharged Coconpsirator-1 ("UCC-1"). Before executing the fraud, UCC-1 took several steps in furtherance of the conspiracy.

10. First, on or about October 5, 2018, UCC-1 founded and organized Company-1, a company which UCC-1 incorporated under the laws of the State of Maryland.[2] The Joint

[1] All dates and amounts throughout this Affidavit are approximate.
[2] On or about October 16, 2020, the State of Maryland changed Company-1's status to forfeited due failure to file a property return in 2019.

Investigation was able to connect Company-1 to UCC-1 through matching addresses found on law enforcement systems, DMV databases, and open-source searches.

11. After incorporating the business, UCC-1 opened the WF-9986 account in the name of Company-1 on October 5, 2018. Based on records subpoenaed from Wells Fargo, the signature card for the WF-9986 account lists two customer names: Company-1 (sole owner) and UCC-1 (signer).

12. The October 2018 statement for the WF-9986 account listed an opening balance of $0.00 and an opening deposit of $25. On October 23, 2018, $20 was withdrawn at an ATM. In November 2018, $10 was debited for "Direct Pay Monthly Base." There were no transactions for November.

13. On December 7, 2018, $20 was credited to the account via a deposit at an ATM at 9800 Apollo Drive, Largo, MD. On December 10, 2018, $356,954 was credited to the account with a description that included Victim-1's name. Given the amount—which matches the amount Victim-1 wired—and the description, this credit likely represents the proceeds of the fraudulent scheme.

14. Debits on December 10, 2018, included $10 due to "Direct Pay Monthly Base" and $15 for a wire service charge. On December 11, 2018, $20 was debited from the account via a withdrawal at an ATM at 9800 Apollo Drive, Largo, MD.

15. On December 11, 2018 and December 12, 2018, almost all of the money was withdrawn from the account as detailed below.

16. On January 24, 2019, the account was closed with the description "Loss Prevention Closing Entry." All told, the WF-9986 account was open for less than four months and had a closing balance of $4 on the date it was closed with the loss prevention entry.

17. Based on my training and experience, the WF-9986 account's transactions are not typical of legitimate business activity. Rather, the small number of transactions, the size of those transactions, and the short timeframe between incoming and outgoing wires suggest fraudulent activity.

C. The Conspirators Transfer the Funds to Other Accounts

18. After receiving responses to a series of grand jury subpoenas, the Joint Investigation determined that the CONSPIRATORS transferred the money to Bank of America and TD Bank accounts controlled by the CONSPIRATORS (collectively, the "Conspirator Accounts"). The Conspirator Accounts include those specified in this Criminal Complaint and additional accounts involved in the scheme.

19. Just after Victim-1 was deceived into wiring $356,954 into the WF-9986 Account, five Wells Fargo Direct Pay debits, totaling $356,900, occurred:

Transactions from the WF-9986 Account			
Date	**Amount**	**Destination Account**	**Associated Defendant**
December 11, 2018	$25,000	BOA-2125 Account	ELKHEBRI, IBEH
December 11, 2018	$50,000	TD-0414 Account	JOYNER
December 11, 2018	$150,000	BOA-4059 Account	AYEAH
December 12, 2018	$31,900	TD-0414 Account	JOYNER
December 12, 2018	$100,000	BOA-4059 Account	AYEAH

20. Each of these transactions involved electronic communication with a server in Minnesota.

i. <u>The BOA-2125 Account Controlled by ELKHEBRI and IBEH</u>

21. A December 11, 2018 transaction of $25,000 was sent to a Bank of America account ending in 2125 (the "BOA-2125 account"). The deposit included a description that referenced Company-1.

22. The signature card for the BOA-2125 account, dated February 8, 2018, listed the owner as ELKHEBRI. The account was opened in the name of a sole proprietorship in ELKHEBRI's name.

23. The BOA-2125 account is linked to two emails: one connected to ELKHEBRI and the other connected to IBEH. The online account access IDs listed for the account also match known aliases of IBEH.[3]

24. Between December 12, 2018, and December 14, 2018, records show outgoing transfers from the BOA-2125 account, including $7,386 in debits via Square, $1,079.95 at the U.S. Postal Service, and $700 in cash.

25. Based on my training and experience, the BOA-2125 account's transactions are not typical of legitimate business activity. Rather, the size of the transactions and the short timeframe between incoming and outgoing wires suggest fraudulent activity.

ii. The BOA-4059 Account controlled by AYEAH.

26. A December 11, 2018 transaction of $150,000 and a December 12, 2018 transaction of $100,000 were sent to a Bank of America account ending in 4059 (the "BOA-4059 account").

27. The signature card for the BOA-4059 account, dated March 23, 2018, lists AYEAH as the sole signer and owner. The BOA-4059 account was opened in the name of a sole proprietorship in AYEAH's name. The BOA-4059 account's listed online account access ID also connects to AYEAH.

28. This account shows a deposit of $150,000 on December 12, 2018, and a deposit of $100,000 on December 13, 2018, and both include a description that references Company-1. These

[3] The online account access IDs are "slick4president" and "slick_4." IBEH's Instagram account name is "slick4president." The Joint Investigation believes the "slick4president" Instagram belongs to IBEH because: (1) the registered email address for the Instagram account matches a known email address of IBEH; and (2) the photographs on the Instagram account match known photographs of IBEH.

amounts match the outgoing transfers on the WF-9986 account, and the amounts were debited from the WF-9986 account on the date immediately preceding their posting to the BOA-4059 account.

29. Records for the BOA-4059 account show this account was debited $120,000 via an international wire to the Bank of Jiangsu[4] and debited $5,000 via an online banking transfer on December 13, 2018. On December 14, 2018, the BOA-4059 account was debited $75,000 via an international wire to the Bank of Jiangsu. On or between December 20, 2018, and December 24, 2018, a total of $7,000 was withdrawn as cash and $10,000 was debited via a wire to LMX Towson, LLC.

30. Based on my training and experience, the BOA-4059's account's transactions are not typical of legitimate business activity. Rather, the size of the transactions, the short timeframe between incoming and outgoing wires, and the international wires suggest fraudulent activity.

iii. The TD-0414 Account Controlled by JOYNER.

31. A December 11, 2018 transaction of $50,000 and a December 12, 2018 transaction of $31,900 was sent to a TD Bank Account ending in -0414 (the "TD-0414 account").

32. The signature card for the TD-0414 account, dated September 7, 2018, lists the owner of the account as JOYNER.

33. Records produced by TD Bank show that the TD-0414 account received a deposit of $50,000 on December 12, 2018, and a deposit of $31,900 on December 13, 2018, both beginning with a description that references Company-1. These amounts match the outgoing transfers on the WF-9986 account, and the amounts were debited from the WF-9986 account on the date immediately preceding their posting to the TD-0414 account.

[4] The Bank of Jiangsu appears to be a commercial bank with an address in Nanjing, China

34. On December 13, 2018, and December 14, 2018, a total of $12,800 was withdrawn from the account as cash via withdrawal tickets. On December 17, 2018, $34,800 was debited from the account via an international outbound wire to the Bank of Jiangsu and $7,500 was withdrawn from the account as cash via a withdrawal ticket. On or between December 12, 2018, and December 17, 2018, additional account debits included $3,725.99 in ATM withdrawals.

35. Based on my training and experience, the TD-0414 account's transactions are not typical of legitimate activity. Rather, the size of the transactions, the short timeframe between incoming and outgoing wires, the international wires, and the large cash withdrawals suggest fraudulent activity.

D. The Investigation Further Ties the Conspirators to the Conspirator Accounts

i. IP Addresses tie IBEH to the Conspirator Accounts

36. In response to legal process, Wells Fargo and Bank of America produced Internet Protocol (IP) logs detailing access to the Conspirator Accounts. The Joint Investigation then subpoenaed the internet service providers for subscriber data for the account holders using the IP addresses. The results included the following:

IP Address Access to the Conspirator Accounts		
IP	*Subscriber Name*	*Service Address*
108.48.27.50	Individual-1 (Connected to IBEH)	7911 Westpark Drive Unit 615 McLean, VA
71.246.208.175	Individual-1 (Connected to IBEH)	5505 Seminary Rd Apt 917 Falls Church, VA
70.110.18.64	Individual-1 (Connected to IBEH)	5505 Seminary Rd Apt 917 Falls Church, VA
71.241.242.143	Individual-1 (Connected to IBEH)	5505 Seminary Rd Apt 917 Falls Church, VA

37. Records show that IP address 108.48.27.50 regularly accessed the BOA-2125 account. According to Verizon, this IP address belongs to Individual-1 at service address 7911 Westpark Dr, Unit 615, McLean, VA. Public records show that Individual-1 and IBEH reside together at this address and have also lived together at the previously mentioned locations too. Furthermore, Individual-1's Virginia driver's license lists their address as 7911 Westpark Dr, Unit 615, McLean, VA.

38. Previous addresses found in public records for Individual-1 include multiple apartments at 5505 Seminary Rd, Falls Church, VA. Therefore, IBEH and/or Individual-1 are likely responsible for the IP logins occurring from IP addresses 71.246.208.175, 70.110.18.64, and 71.241.242.143. Taken together with the other evidence, the Joint Investigation believes IBEH controlled and accessed the Conspirator Accounts.

ii. Surveillance Footage Ties JOYNER to the Conspirator Accounts

39. In response to legal process, TD Bank produced surveillance footage of certain ATM transactions involving the TD-0414 account, including ATM transactions occurring in the Eastern District of Virginia. At least one of these transactions features an individual who matches the known height, weight, and body type description of JOYNER. The Joint Investigation compared photographs of the person seen on surveillance footage conducting the transactions to known photographs of JOYNER taken from law enforcement databases. These appear to be the same person. Taken together with the other evidence, the Joint Investigation believes JOYNER controlled and accessed the TD-0414 account.

iii. Surveillance Footage Ties AYEAH to the Conspirator Accounts

40. In response to legal process, Bank of America produced surveillance footage of certain ATM transactions involving the BOA-4059 account and other Conspirator Accounts.

Several of these transactions feature an individual who matches the known height, weight, and body type description of AYEAH. The Joint Investigation compared photographs of the person seen on surveillance footage conducting the transactions to known photographs of AYEAH. These appear to be the same person. Taken together with the other evidence, the Joint Investigation believes AYEAH controlled and accessed the BOA-4059 account and other Conspirator Accounts.

iv. Employment Records Tie ELKHEBRI to the Conspirator Accounts

41. In response to legal process, Bank of America produced personnel records for ELKHEBRI, who worked as a personal banker and relationship manager there from 2015 until 2017. During his time at Bank of America, ELKHEBRI opened multiple Conspirator Accounts, including an account that IBEH used in furtherance of the scheme.

42. In response to legal process, TD Bank also produced personnel records for ELKHEBRI, who worked there from 2017 until 2018. During his time at TD Bank, ELKHEBRI opened multiple Conspirator Accounts, including an account that AYEAH used in furtherance of the scheme. Additionally, ELKHEBRI opened a Conspirator Account for Uncharged Coconspirator-2 (UCC-2) who, days later, paid $1,000 to a Square cash account that resembles ELKHEBRI's name.

E. The CONSPIRATORS Defraud Additional Victims.

i. Victim-2

43. On or about December 5, 2018, a victim located in Dallas, Texas ("Victim-2"), filed a complaint stating that their business was defrauded of $256,776.23 over three transactions: $93,039.24 on September 4, 2018; $121,878.56 on October 1, 2018; and $41,858.43 on October 31, 2018. This information was confirmed on or about November 20, 2019, when the Joint Investigation interviewed Victim-2. Unlike Victim-1, Victim-2 was meant to be the legitimate

funds recipient and their business partner was deceived to wiring funds from their HSBC account in the Kingdom of Bahrain to a CONSPIRATOR-controlled Wells Fargo account ending in -7282 (the "WF-7282 account"). According to Victim-2, the email deception was accomplished by the CONSPIRATORS registering a domain name with a misspelling (*i.e.* a look-a-like domain) and compromising the email communications of their business partners.

44. Records from Wells Fargo show that the WF-7282 account was opened by Uncharged Coconspirator-3 ("UCC-3") in the name of Company-2.[5] From August 29, 2018 to September 6, 2018, the WF-7282 account received four credits via wire, including $93,039.24 which matches the amount sent by Victim-2.[6] Ultimately, the funds from Victim-2 were transferred to other conspirators:

Transactions from the WF-7282 Account[7]			
Date	**Amount**	**Destination Account**	**Associated Defendant**
September 10, 2018	$60,000	BOA-2125 Account	ELKHEBRI, IBEH
September 10, 2018	$140,000	BOA-4059 Account	AYEAH
September 11, 2018	$33,000	BOA-2125 Account	ELKHEBRI, IBEH
September 11, 2018	$80,000	BOA-4059 Account	AYEAH

ii. Victim-3

45. On or about May 18, 2019, a victim located in Chula Vista, California ("Victim-3"), filed a complaint stating that their business was defrauded of $114,757.59 on April 16, 2019. This information was confirmed on or about January 6, 2020, when the Joint Investigation interviewed Victim-3's CEO. Similar to Victim-2, Victim-3 was meant to be the legitimate funds recipient and their business partner was deceived into wiring funds to a CONSPIRATOR-controlled account. Victim-3's business partner sent the funds from their HSBC account in Hong

[5] On or about July 27, 2018, UCC-3 founded and organized Company-2, a company incorporated under the laws of the State of Maryland.
[6] The additional wires were for $17,174.04, $3,200 and $200,000 and totaled $313,300.
[7] These are the same accounts that the CONSPIRATORS used to affect the fraud against Victim-1.

Kong to a CONSPIRATOR-controlled Wells Fargo account ending in -6217 (the "WF-6217 account"). According to Victim-3, the email deception was accomplished by the CONSPIRATORS using an email similar to his email and compromising the email communications of the business partners.

46. Records from Wells Fargo show that the WF-6217 account was opened by Uncharged Coconspirator-4 ("UCC-4") in the name of Company-3.[8] On April 16, 2019, the WF-6217 account was credited $114,757.59 via wire, which matches the amount sent by Victim-3. Ultimately, the funds from Victim-3 were transferred to other conspirators:

Transactions from the WF-6217 Account			
Date	**Amount**	**Destination Account**	**Associated Defendant**
April 19, 2019	$110,000	BOA-4059 Account	AYEAH
April 19, 2019	$4,000	BOA-2500	UCC-5

iii. Victim-4

47. On or about July 27, 2018, a victim located in Falls Church, Virginia, within the Eastern District of Virginia ("Victim-4") filed a complaint stating that their business was defrauded of a total of $126,348.66 in two transactions: $63,174.22 on July 3, 2018, and $63,174.22 on July 25, 2018. This information was confirmed on or about October 29, 2019, when the Joint Investigation interviewed Victim-4's President. Similar to Victim-2 and Victim-3, Victim-4 was meant to be the legitimate funds recipient and their business partner was deceived into wiring the funds to a CONSPIRATOR-controlled account. Victim-4's business partner sent the funds from their account in Chile to CONSPIRATOR-controlled Wells Fargo accounts ending in -8532 (the "WF-8532 account") and -5753 (the "WF-5753 account"). Victim-4 stated that the email deception was accomplished by the CONSPIRATORS impersonating him via email to his business partner.

[8] On or about March 13, 2019, UCC-4 incorporated Company-3 under the laws of the State of Maryland.

Victim-4 did not believe that his business partner was impersonated in communications directed to his company.

48. Records from Wells Fargo show that the WF-8532 account was opened by Uncharged Coconspirator-5 ("UCC-5") in the name of Company-4.[9] On July 2, 2018, the WF-8532 account was credited $63,174.33. The wire details match the name of the business partner of Victim-4 and the amount sent. Ultimately, the funds from Victim-4 were transferred to other conspirators:

Transactions from the WF-8532 Account[10]			
Date	**Amount**	**Destination Account**	**Associated Defendant**
June 4, 2018	$10,300	BOA-2125 Account	ELKHEBRI, IBEH
June 4, 2018	$35,000	BOA-4059 Account	AYEAH
June 13, 2018	$20,000	BOA-2125 Account	ELKHEBRI, IBEH
June 13, 2018	$120,000	BOA-4059 Account	AYEAH
July 3, 2018	$8,100	BOA-2125 Account	ELKHEBRI, IBEH
July 3, 2018	$55,000	BOA-4059 Account	AYEAH

* * *

[9] On or about May 23, 2018, UCC-5 founded and organized Company-4, a company which UCC-5 incorporated under the laws of the Commonwealth of Virginia.

[10] These are the same accounts that the CONSPIRATORS used to affect the fraud against Victim-1.

CONCLUSION

49. Based on the information contained herein, I respectfully submit that there is probable cause to believe ANTHONY AYEAH ("AYEAH"); MOUAAZ ELKHEBRI ("ELKHEBRI"); ONYEWUCHI IBEH ("IBEH"); and JASON JOYNER ("JOYNER") (collectively, the "CONSPIRATORS") from on or about March 23, 2018, to on or about March 31, 2020, in the Eastern District of Virginia, and elsewhere, knowingly and intentionally conspired with others to commit wire fraud by: (a) knowingly devising and intending to devise a scheme and artifice to defraud and to obtain money by means of materially false and fraudulent pretenses, representations, and promises; and (b) transmitting and causing to be transmitted interstate wire communications in furtherance of the conspiracy, in violation of Title 18, United States Code, Section 1343 and Title 18, United States Code, Section 1349.

EDPAPISH Digitally signed by EDPAPISH Date: 2021.08.06 12:17:42 -04'00'

Ethan Papish
Special Agent
United States Secret Service

Reviewed by: William Fitzpatrick, Assistant United States Attorney
Christopher J. Hood, Assistant United States Attorney

Sworn to and subscribed in accordance with Fed. R. Crim. P. 4.1 by telephone on this 10th day of August 2021.

Digitally signed by Michael S. Nachmanoff
Date: 2021.08.10 11:31:15 -04'00'

The Honorable Michael S. Nachmanoff
United States Magistrate Judge